Running head: Hyperelliptic class groups
Math. Subj. Class. (1991): 11R29, 14H40

December 16, 1998
(slightly revised, August 25, 1999)

The 2-primary class group of certain hyperelliptic curves

by Gunther Cornelissen

Introduction

In a letter to Dirichlet, dated May 30, 1828 ([5]), Gauß considered the divisibility of the class number of $\mathbf{Q}(\sqrt{-p})$ (p prime, $= 1 \bmod 4$) by 8. Many variations on this theme can be found in the mathematical literature of the subsequent centuries, either using quadratic forms or class field theory (Rédei [15], Barrucand-Cohn [3], Hasse [10], Kaplan [12], Stevenhagen [17]). Of these, the latter approach seems to give the most dense and structural arguments. To understand Gauß' letter from this point of view, one makes essential use of the fact that the 2-primary part of the class group is cyclic, and that the 2-torsion in the class group of $\mathbf{Q}(\sqrt{-p})$ is generated by the prime ideal above 2. In particular, the norm of the ambiguous class is independent of p. The divisibility of the class number by 16 or even higher powers of 2 seems to be less tractable.

In the twenties, E. Artin in his thesis ([2]) developed an arithmetic theory of quadratic extensions of the rational function field over a finite field, which shows a remarkable resemblance to the classical works of Gauß (quadratic forms), Dirichlet-Minkowski (units), Kummer-Dedekind (ideal class groups) and Riemann (zeta functions). With his terminology at hand, one can ask for the obvious analogue of the above: when is the class number of (the ring of integers of) an imaginary hyperelliptic function field divisible by 2, 4 or 8?

Throughout, we will assume that the characteristic of the ground field is different from 2. The 2-power rank of Artin-Schreier curves over fields of characteristic 2 was studied by van der Geer and van der Vlugt ([6]).

In view of arithmetic algebraic geometry, one has a lot of additional geometric structure to study our question. The link between the class group and the Jacobian of the corresponding curve is well known (see the proof of the first corollary below). In particular, one can use the action of Galois on the 2-power torsion in the Jacobian of the curve. Such an approach was undertaken in section 5 of [4] (following the suggestion of a referee), and leads to a very satisfactory answer. But one can still wonder whether a class field theory approach to the problem is possible, and this is what we will attempt in this note. The geometric result on the existence of rational torsion points on Jacobians of certain hyperelliptic curves then comes out "for free". The main results can be stated as follows:

Theorem 1. *Fix a non-square $e \in \mathbf{F}_q$. For a prime $\mathfrak{p}$ of $\mathbf{F}_q[T]$, the class number of (the Dedekind ring) $\mathbf{F}_q[T, \sqrt{e\mathfrak{p}}]$ is even if and only if* $\deg \mathfrak{p}$ *is, and is divisible by 4 if and only if* $\deg \mathfrak{p}$ *is.*

Theorem 2. *If k is a fixed integer divisible by 4, then there exists a constant C_k such that for all prime powers $q > C_k$ coprime to $k-4$, there exist two primes $\mathfrak{p}$ and $\mathfrak{p}'$ of degree k in $\mathbf{F}_q[T]$ and non-squares e, e' in $\mathbf{F}_q$ such that the class numbers of $\mathbf{F}_q[T, \sqrt{e\mathfrak{p}}]$ and $\mathbf{F}_q[T, \sqrt{e'\mathfrak{p}'}]$ are different modulo 8.*

Corollary 1. *Let $J(e\mathfrak{p})$ be the Jacobian of a non-singular projective hyperelliptic curve whose affine equation is $y^2 = e\mathfrak{p}$ for some non-square $e \in \mathbf{F}_q$ and an irreducible polynomial $\mathfrak{p}$ of degree k in $\mathbf{F}_q[T]$. Then $J(e\mathfrak{p})$ has an $\mathbf{F}_q$-rational two-torsion point if and only if k is divisible by 4. Furthermore, for $4|k$ and all prime powers $q > C_k$ coprime to $k-4$ there are two irreducible $\mathfrak{p}$ and $\mathfrak{p}'$ of degree k and e, e' non-squares in $\mathbf{F}_q$ such that $J(e\mathfrak{p})$ (resp. $J(e'\mathfrak{p}')$) does (resp. does not) have an $\mathbf{F}_q$-rational point of exact order 4.*

Corollary 2. *Let k be an integer divisible by 4. For all prime powers $q > C_k$ coprime to $k-4$, there exists two quaternion algebras over $\mathbf{F}_q(T)$ which are both ramified only at infinity (T^{-1}) and a unique finite prime of degree k in $\mathbf{F}_q[T]$, but whose type numbers (the number of non-conjugate maximal orders) have different parity.*

Contrary to the case of rational integers, the ambiguous class of hyperelliptic function fields *does* depend on the discriminant, and this turns out to be a severe obstruction to an immediate translation of the classical argument. It also obscures the classical construction of a governing field for the 8-rank.

Recall that a Galois extension Ω_r of $\mathbf{F}_q(T)$ is called a governing field for the 2^r-rank with multiplier e if for all irreducible $\mathfrak{p} \in \mathbf{F}_q[T]$, the class number of $\mathbf{F}_q(T, \sqrt{e\mathfrak{p}})$ is divisible by 2^r if and only if $\mathfrak{p}$ splits in Ω_r (with Ω_r independent of $\mathfrak{p}$). From theorem 1, we see that Ω_2 and Ω_4 exist and are just the constant extensions $\mathbf{F}_{q^2}(T)$ and $\mathbf{F}_{q^4}(T)$. It is classically known that the 8-rank of $\mathbf{Q}$-extensions with multiplier -1 is governed by $\mathbf{Q}(\sqrt[8]{-1}, \sqrt{i+1})$; its construction depends heavily on the aforementioned independence (*cf.* [17] and the references therein). The analogue of this for $\mathbf{F}_q(T)$ is less clear: *does there exist a field governing the 8-rank of class groups of hyperelliptic curves?* Let us only note that Bauer's theorem ("Galois extensions of number fields are determined by their splitting primes", *cf.* Neukirch [13] VII.13.9) remains true for function fields up to constant extensions. This implies that $\Omega_r \otimes \bar{\mathbf{F}}_q \subseteq \Omega_{r+1} \otimes \bar{\mathbf{F}}_q$.

The plan of this note is as follows: we recall the genus theory of Artin and its connection to the parity of the class number. We then provide a class field theory approach to 4-divisibility. However, we also give a second short argument using Drinfeld modular curves. Taken the construction of certain special ambiguous classes for granted, we use class field theory to formulate a criterium for 8-divisibility of the class number of curves corresponding to these classes. In the next paragraph, discriminants having appropriate ambiguous classes are constructed; to produce them, we construct certain "lifts" of the coefficients of $\mathfrak{p}$ to the function field $\mathbf{F}_q(t)$ and rely on Chebotarëv's density theorem. Thus, the constant C_k can be effectively estimated, and then the explicit construction of $\mathfrak{p}$ and $\mathfrak{p}'$ is easy from the given data. The final paragraph is devoted to the proof of the corollaries.

By similar constructions, it ought to be possible to surpress the divisibility conditions imposed on q and $k-4$ in theorem 2.

The results of this paper grew out of an attempt to get a better understanding of the interrelations between such class numbers, supersingular Drinfeld modules and Eisenstein series. For applications in that sense, see [4].

1. Notations – Genus theory (E. Artin [2], section 11)

Let $\mathbf{F}_q$ be a finite field with q elements of characteristic $p \neq 2$, and let $K := \mathbf{F}_q(T)$ be the rational function field over $\mathbf{F}_q$ with maximal T^{-1}-order $A = \mathbf{F}_q[T]$. Let e be a non-square in $\mathbf{F}_q$, and $\mathfrak{p}$ an irreducible non-constant polynomial of degree k in A. We write $L = K(\sqrt{e\mathfrak{p}})$ for the quadratic extension of K of discriminant $e\mathfrak{p}$, and $\mathcal{O}$ for its ring of integers. L is a so-called *imaginary* quadratic extension of K since T^{-1} is inert in L.

Let $h(e\mathfrak{p})$ denote the class number of $\mathcal{O}$. Let $\mathcal{C}$ denote the 2-primary part of the divisor class group of the Dedekind ring $\mathcal{O}$. Then $\mathcal{C}$ is a cyclic 2-group (since the discriminant has only one monic prime divisor), and it is trivial if and only if $\deg(\mathfrak{p})$ is odd (*cf.* Artin, section 11, Satz). This proves the first claim in theorem 1.

Artin also shows that if $\deg(\mathfrak{p})$ is even, then the two-torsion of $\mathcal{C}$ is generated by the "ambiguous class" $\mathcal{A}$, constructed as follows: consider the quadratic form

$$\kappa(X,Y) = eX^2 + \alpha XY + Y^2,$$

where $\alpha \in \mathbf{F}_q$ is chosen such that κ is irreducible over $\mathbf{F}_q$. If $(B,C) \in A$ are such that

$$e\mathfrak{p} = \kappa(B,C) \text{ with } \deg B < \deg C = \frac{k}{2},$$

then in fact $\mathcal{A}$ is the class of the ideal $(C, B+\sqrt{e\mathfrak{p}})$. A small computation shows that it has K-norm $N_K^L(\mathcal{A}) = C$. As we have remarked in the introduction, this norm depends on the discriminant of L. If $\mathfrak{p}$ corresponds to B and C in this way, we will indicate this dependence by $\mathfrak{p}(B,C)$, by slight abuse of notation.

Let H be the Hilbert class field of L; this means the maximal abelian unramified extension of L in which T^{-1} is totally split ([11]). We will let $\mathcal{C}^i$ denote the groups $\{c^i | c \in \mathcal{C}\}$. We will denote by H_i the fixed field of H under $\mathcal{C}^i$. Because of the cyclic structure of $\mathcal{C}$, we see that

$$2^i | h(e\mathfrak{p}) \iff [H_{2^i} : L] = 2^i.$$

2. Proof of theorem 1

(2.1) *Proof using class field theory.* The parity of the class number is given by the genus theory of §1. For the divisibility by 4, assume that $k = \deg(\mathfrak{p})$ is even, *viz.* $[H_2 : L] = 2$. The class number $h(e\mathfrak{p})$ of $\mathcal{O}$ is divisible by 4 if and only if $[H_4 : H_2] = 2$. We will use properties of the subfield $K(\sqrt{e})$, which is independent of $\mathfrak{p}$. This is actually the exact field of constants of H_4, so that in what follows we will not have to worry about unramified extensions of $K(\sqrt{e})$ in H_4. Since the "genus field" H_2 equals $L(\sqrt{e})$, 4 divides $h(e\mathfrak{p})$ if and only if $[H_4 : K(\sqrt{e})] = 4$.

The extension $H_4/K(\sqrt{e})$ is unramified outside $\mathfrak{p}$, and hence a subextension of the ray class field of $K(\sqrt{e})$ modulo $\mathfrak{p}$. Let $R_\mathfrak{p}$ be the ray class group of $K(\sqrt{e})$ at $\mathfrak{p}$. Then $\mathrm{Gal}(H_4/K(\sqrt{e}))$ is a quotient of $R_\mathfrak{p}$. Since $K(\sqrt{e})$ has class number one, it equals its own class field. If $\mathfrak{p}$ splits as $\pi.\pi'$ in $K(\sqrt{e})$, then $R_\mathfrak{p}$ is by class field theory equal to

$$R_\mathfrak{p} = [(A[\sqrt{e}]/\pi)^* \times (A[\sqrt{e}]/\pi')^*]/\mathbf{F}_q^*(\sqrt{e}). \tag{2.1.1}$$

(see Hayes, [11] §9). The situation is summarized in the following diagram:

$$\begin{tikzcd}
& H_4 \arrow[d, dash, "?\ 1\text{ or }2"'] \arrow[ddr, dash, "R_\mathfrak{p}/R_\mathfrak{p}^2,\ (?\ 2\text{ or }4)"] & \\
& H_2 \arrow[dl, dash, "2"'] \arrow[dr, dash] & \\
L = K(\sqrt{e\mathfrak{p}}) \arrow[dr, dash, "2"'] & & K(\sqrt{e}) \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

From this diagram, we see that the Galois group of the extension $H_4/K(\sqrt{e})$ is of exponent 2, and hence a surjective image of $R_\mathfrak{p}/R_\mathfrak{p}^2$.

If 4 divides $h(e\mathfrak{p})$, then $[H_4 : K(\sqrt{e})] = 4$, so $R_\mathfrak{p}/R_\mathfrak{p}^2$ has order 4. By (2.1.1), this means that $\sqrt{e}$ is a square modulo π. But that happens if and only if $2 | \deg(\pi)$, *viz.*, $4|k$.

On the other hand, if $4|k$, then $R_\mathfrak{p}/R_\mathfrak{p}^2$ has order 4. To it corresponds an extension of $K(\sqrt{e})$ with Galois group $\mathbf{Z}/2 \times \mathbf{Z}/2$ by (2.1.1), which is only ramified at the primes above $\mathfrak{p}$, at most with ramification index 2. Hence it is contained in H_4. But then $[H_4 : K(\sqrt{e})] \geq 4$, *i.e.*, 4 divides $h(e\mathfrak{p})$. □

(2.2) *Proof using modular curves.* Let k again be even. In [7], E.-U. Gekeler shows that

$$4g(\mathfrak{p}) = 2\frac{q^k - 1}{q^2 - 1} + h(e\mathfrak{p}),$$

where $g(\mathfrak{p})$ is an integer. Let it suffice for the *cognoscenti* to remark that $g(\mathfrak{p})$ is the genus of the quotient of the Drinfeld modular curve $X_0(\mathfrak{p})$ by the $\mathfrak{p}$-Atkin-Lehner involution, or equivalently, the number of quadratic j-invariants for rank-two Drinfeld modules that are supersingular modulo $\mathfrak{p}$.

Since it is elementary to see that $2(q^k-1)/(q^2-1) = k \bmod 4$, we again find that $4|h(e\mathfrak{p})$ if and only if $4|k$. $\square$

3. Proof of theorem 2

(3.1) The cyclic structure of $\mathcal{C}$ implies that $h(e\mathfrak{p})$ is divisible by 8 if and only if $\mathcal{A} \in \mathcal{C}^4$. We will now proceed to construct, for k divisible by 4 and q large enough, a pair (B, C) of a particular form, and derive a criterium for the corresponding field $K(\sqrt{e\mathfrak{p}(B,C)})$ to have class groups of prescribed 8-rank. *Throughout this section, we set* $l = k/2$ (which is even), and use the notations of the first paragraph. It will also be useful to keep in mind the diagram of §2.

(3.2) Let $C = T^{l-2}Q(T)$ for some quadratic irreducible polynomial $Q(T) = T^2 + aT + b$ over $\mathbf{F}_q$, and let $B = b_0T^{l-2} + b_1 \in A$. Write $L = K(\sqrt{e\mathfrak{p}(B,C)})$. It is easy to see that all factors of C split in L/K, since $e\mathfrak{p} = B^2 \bmod C$ and the conductor of $A[e\mathfrak{p}]$ is trivial. Hence we can write $T = \mathcal{T}\mathcal{T}'$ and $Q = \mathcal{Q}\mathcal{Q}'$ in L. Then the ambiguous class is $\mathcal{A} = \mathcal{T}^{l-2}\mathcal{Q}$.

Since T is of degree one, it is not split in the (constant) extension $K(\sqrt{e}) = \mathbf{F}_{q^2} \otimes K$. Since the ramification index and residue class degree of T in H_2/K are the same whether computed via L or via $K(\sqrt{e})$, we find that $\mathcal{T}$ is not split in H_2/L either, *i.e.*, $\mathrm{Frob}_{\mathcal{T}} \neq 1$ in $\mathrm{Gal}(H_2/L) = \mathcal{C}/\mathcal{C}^2$. On the other hand, Q splits in $K(\sqrt{e})/K$, say as $Q = \mathcal{L} \cdot \mathcal{L}'$, and one sees that $\mathcal{L}$ and $\mathcal{L}'$ also split in $H_2 = L(\sqrt{e})/K(\sqrt{e})$ (again since $e\mathfrak{p}$ is a square modulo $\mathcal{L}$). Hence by a similar argument as before, $\mathcal{Q}$ splits in H_2/L, *i.e.*, $\mathrm{Frob}_{\mathcal{Q}} = 1$ in $\mathrm{Gal}(H_2/L)$. If we let σ denote a generator of the cyclic group $\mathrm{Gal}(\varinjlim H_{2^i}/L) \cong \mathcal{C}$, then we can write $\mathrm{Frob}_{\mathcal{T}}^2 = \sigma^{4m+2}$, and $\mathrm{Frob}_{\mathcal{Q}} = \sigma^{2n}$ for some $m, n \in \mathbf{Z}$. We now distinguish two cases:

(3.2.1) *First case: $l-2$ is divisible by 4.* The class number $h(e\mathfrak{p})$ is divisible by 8 if and only if $\mathcal{A} \in \mathcal{C}^4$, *i.e.*, $\mathrm{Frob}_{\mathcal{T}}^{\frac{l-2}{2}} \circ \mathrm{Frob}_{\mathcal{Q}} = 1$ in $\mathrm{Gal}(H_4/L)$. Since the latter group is of exponent 4, this is equivalent to $\mathrm{Frob}_{\mathcal{Q}}$ acting trivial in $\mathrm{Gal}(H_4/L)$. So we want $\mathcal{Q}$ to split completely in H_4/L. But this is equivalent to $\mathcal{L}$ splitting completely in $H_4/K(\sqrt{e})$ (then the same follows for $\mathcal{L}'$). Using the description of its Galois group in terms of the ray class group at $\mathfrak{p}$ given earlier, we want that $\mathrm{Frob}_{\mathcal{L}}$ acts trivial in $R_{\mathfrak{p}}/R_{\mathfrak{p}}^2$. Writing $\mathfrak{p} = \pi\pi'$ in $K(\sqrt{e})$ as before, and using (2.1.1), this is equivalent to $\mathcal{L}$ being a square modulo π in $\mathbf{F}_{q^2}$ (the same then immediately holds modulo π' since $\mathfrak{p}$ is a square modulo $\mathcal{L}$).

We can reformulate this criterium using quadratic residue symbols $(\dot{\bar{\cdot}})$ for $\mathbf{F}_{q^2}(T)$ as follows. Let us factor the quadratic form κ over $\mathbf{F}_{q^2}$ as

$$\kappa(X,Y) = e(X - \delta Y)(X - \bar{\delta}Y) \text{ over } \mathbf{F}_{q^2},$$

where $2e\delta = \alpha \pm \sqrt{\alpha^2 - 4e}$. Then $\pi = C - \delta B = T^{l-2}Q(T) - \delta B(T)$ for some choice of δ. Let λ be an root of Q in $\mathbf{F}_{q^2}$, say, $\mathcal{L} = T - \lambda$. Our criterium reads

$$\begin{aligned} 8|h(e\mathfrak{p}) \quad &\Longleftrightarrow \quad (\frac{\mathcal{L}}{\pi}) = 1 \Longleftrightarrow (\frac{\pi}{\mathcal{L}}) = 1 \\ &\Longleftrightarrow \quad \delta B(\lambda) = \text{ square in } \mathbf{F}_{q^2}, \end{aligned}$$

using quadratic reciprocity and the fact that $\mathcal{L}$ is a factor of Q.

(3.2.2) *Second case: l is divisible by 4.* Now, the class number $h(e\mathfrak{p})$ is divisible by 8 if and only if $\mathrm{Frob}_T^2 \circ \mathrm{Frob}_Q = 1$ in $\mathrm{Gal}(H_4/L)$, *viz.*, $\sigma^{4m+2+2n} = 1$ in $\mathrm{Gal}(H_4/L)$. Since the latter group is of exponent 4, this happens if and only if n is odd, *i.e.*, $\mathrm{Frob}_Q \neq 1$ in $\mathrm{Gal}(H_4/L)$. We can then follow the argument of (3.2.1) to see that this is equivalent to

$$8|h(e\mathfrak{p}) \Longleftrightarrow \delta B(\lambda) \neq \text{ square in } \mathbf{F}_{q^2}.$$

(3.3) For the above constructions to work, we have to require additionally that $\mathfrak{p}(B, C)$ is irreducible over $\mathbf{F}_q$, and that e is a non-square in $\mathbf{F}_q$. Factor κ as before. The fact that $\kappa(0,1) = 1$ implies that $\delta\bar{\delta} = e^{-1}$. In the next section we will prove the following proposition:

(3.4) Proposition. *Fix an even integer l. There is a constant C_l such that for all prime powers $q > C_l$ coprime to $l-2$, there exists a quadratic irreducible Q over $\mathbf{F}_q$, $B^{\pm}(T) = b_0^{\pm}T^{l-2} + b_1^{\pm} \in \mathbf{F}_q[T]$ and $\delta^{\pm} \in \mathbf{F}_{q^2}$ such that*

$$T^{l-2}Q(T) - \delta^{\pm}B^{\pm}(T)$$

is irreducible over $\mathbf{F}_{q^2}$, and such that $B^{-}(\lambda)$ is (and $\delta^{\pm}$ and $B^{+}(\lambda)$ are not) a square in $\mathbf{F}_{q^2}$, where λ is a root of Q in $\mathbf{F}_{q^2}$.

Let us show how this leads to our requirements. Remark that once $\delta^{\pm}$ is given, it is easy to compute a corresponding α. Since $\delta^{\pm}$ is not a square in $\mathbf{F}_{q^2}$, the inverse of its norm, e, is not a square in $\mathbf{F}_q$. Also, since $\delta^{\pm} \notin \mathbf{F}_q$, the corresponding $\mathfrak{p}$ is irreducible. Namely, if $C - \delta^{\pm}B^{\pm} \in \mathbf{F}_q[T]$, then it would factor over $\mathbf{F}_{q^2}$ since its degree l is even. $\square$

4. Construction of appropriate discriminants

(4.1) Proposition. *Let q be an odd prime power and l an even integer such that $l-2$ is coprime to q. Let $Q(T) = T^2 + aT + b$ be an irreducible quadratic polynomial over $\mathbf{F}_q$ with $a \neq 0$. Let $B(T) = b_0T^{l-2} + b_1$ be an irreducible polynomial in $\mathbf{F}_q[T]$ with $b_0, b_1 \neq 0$. Assume that $B(\lambda) \neq 0$ for the roots λ of Q. Then the polynomial*

$$f := T^{l-2}Q(T) - tB(T)$$

has Galois group S_l over $\mathbf{F}_{q^2}(t)$ and its splitting field has $\mathbf{F}_{q^2}$ as its exact field of constants.

Proof. We see that f is irreducible over $\mathbf{F}_p(t)$ using Gauß' lemma since it is irreducible as a (linear) polynomial in t. Let G be its Galois group over $\mathbf{F}_{q^2}(t)$.

We will first prove that G is primitive. Remark that it suffices to show that G is 2-transitive ([18], Theorem 9.6). For this, it suffices to show that the stabilizer of any root α of f is transitive. We now appeal to the following "twisted derivative"-trick of Abhyankar's ([1], §18), which says that this stabilizer is

$$\mathrm{Gal}(F/\mathbf{F}_{q^2}(\alpha)), \text{ where } F = \frac{f(T) - f(\alpha)}{T - \alpha}.$$

If we compute F using $t = \alpha^{l-2} Q(\alpha) B(\alpha)^{-1}$, we get

$$F = T^{l-1} + (\alpha + a) T^{l-2} + b_1 \frac{Q(\alpha)}{B(\alpha)} \sum_{i=0}^{l-3} \alpha^i T^{l-3-i}.$$

All we have to show is that F is irreducible over $\mathbf{F}_{q^2}(\alpha)$, which is a rational function field (remark that α is transcendental over $\mathbf{F}_{q^2}$). The Newton polygon for the valuation corresponding to the prime factors of $Q(\alpha)$ in $\mathbf{F}_{q^2}[\alpha]$ contains a straight line segment from $(0,1)$ to $(l-2,0)$ which goes through no integer lattice points. Hence if F is reducible, it has a root, say T_0, which is not divisible by any factor of $Q(\alpha)$. By assumption, $B(\alpha)$ has at most two factors over $\mathbf{F}_{q^2}[\alpha]$, and the Newton polygon of F for such a factor is a straight line from $(0,-1)$ to $(l-2,1)$ followed by a segment of slope one. Hence such a factor of $B(\alpha)$ occurs at most once in the factorization of T_0. From the Newton polygons of F for all other finite valuations, one sees that the only possible further divisor of T_0 is α, with valuation -1. The Newton polygon of F for the valuation $-\deg_\alpha$ is a straight line from $(0,-1)$ to $(l-2,-1)$ having slope zero, followed by a segment from $(l-2,-1)$ to $(l-1,0)$ having slope one. Since F has no constant roots, we find that $\deg_\alpha T_0 = 1$. Suppose first that $l \neq 4$. Then a factor of $B(\alpha)$ (which has degree $\frac{1}{2}(l-2) > 1$) cannot divide T_0. The data just computed imply that T_0 is constant, a contradiction. Similarly, if $l = 4$, let β_1, β_2 denote the two (linear) factors of B over $\mathbf{F}_{q^2}$. Then the only possibilities are that T_0 is a scalar multiple of $\beta_1(\alpha), \beta_2(\alpha)$ or $B(\alpha)\alpha^{-1}$. If we expand the two leading terms of $F(T_0)$ in α in each of these cases, we find that β_1, β_2 are defined over $\mathbf{F}_q$, which contradicts the supposed irreducibility of B over $\mathbf{F}_q$.

We will now prove that G contains a 2-cycle. Make the following change of variables: $Y = 1/T, u = 1/t$. Then

$$f = b_1 Y^l + b_0 Y^2 - u(bY^2 + aY + 1).$$

This is an Eisenstein polynomial for the prime u, and its reduction is $f = Y^2(b_1 Y^{l-2} + b_0) \bmod u$. Since $b_0 Y^{l-2} + b_1$ has no multiple roots over $\mathbf{F}_{q^2}$, the factorization of f over the u-completion of $\mathbf{F}_{q^2}(t)$ consists of an Eisenstein polynomial of degree 2 multiplied by a polynomial without multiple factors mod u. Proposition (3.1) in [4] says that the inertia group of the splitting field of an Eisenstein polynomial over a local field whose degree, say N, is prime to the residue characteristic contains an N-cycle. If we apply it to our situation, we find that the inertia group of $1/t$ in G contains a 2-cycle.

We now appeal to a result of Jordan ([14]) which says that a primitive permutation group of degree l containing a 2-cycle is $(l-1)$-transitive. Hence $G = S_l$.

If $\mathbf{F}_{q^{2N}}$ is the exact field of constants of the splitting field $\mathcal{F}$ of f over $\mathbf{F}_{q^2}$, then $\mathbf{F}_{q^{2N}}(t)$ is the fixed field of the group G' generated by all inertia groups. Since A_l is simple for $l > 4$, we find that G' is either A_l or S_l. But above we have constructed an even element in such an inertia group, so this proves that $N = 1$ in those cases. If $l = 4$, then the only other normal subgroup of A_l is generated by products of two transpositions, but this group can also not equal G' since the latter contains a transposition. □

(4.2) *Proof of proposition (3.4).* Choose $Q = T^2 + aT + b$ irreducible over $\mathbf{F}_q$ with $a \neq 0$, having a root λ which is a multiplicative generator for $\mathbf{F}^*_{q^2}$. Choose q big enough to have $q + 1 > l - 2$. Then $\lambda^{l-2} \notin \mathbf{F}_q$. This implies that the set $\{b_0\lambda^{l-2} + b_1 : b_0, b_1 \in \mathbf{F}_q\}$ is the whole of $\mathbf{F}_{q^2}$. Hence we can choose $B^{\pm}$ such that $B^{-}(\lambda)$ is (and $B^{+}(\lambda)$ is not) a square in $\mathbf{F}_{q^2}$ (with the corresponding $b_i^{\pm} \neq 0$) by imposing one linear relation between b_0 and b_1. Also, one can choose such $b_0^{\pm}, b_1^{\pm}$ such that $B^{\pm}(T)$ is irreducible over $\mathbf{F}_q[T]$ (this is the easy case of the Hansen-Mullen conjecture, *cf.* [9]). Let $f^{\pm} = T^{l-2}Q(T) - tB^{\pm}(T)$. By the previous proposition, we find that the splitting field $\mathcal{F}^{\pm}$ of $f^{\pm}$ over $\mathbf{F}_{q^2}(t)$ has an l-cycle σ_l in its Galois group, and $\mathbf{F}_{q^2}$ as its exact field of constants.

There are now two possibilities: either the Galois group of $f^{\pm}$ over $\mathbf{F}_{q^2}(\sqrt{t})$ is A_l or S_l, depending on whether the discriminant of $f^{\pm}$ equals t up to squares or not. Suppose it is A_l. We can apply Chebotarëv's theorem (as in the appendix of Geyer and Jarden [8]) to the Galois extension $\mathcal{F}^{\pm}$ of $\mathbf{F}_{q^2}(t)$ to find that for big enough q, there exists primes $P^{\pm} = t - \delta^{\pm}$ of degree one in $\mathbf{F}_{q^2}(t)$ whose Frobenius elements act like the l-cycle σ_l on the roots of $f^{\pm}$. Since $\mathbf{F}_{q^2}(\sqrt{t})$ is the fixed field of A_l in $\mathcal{F}^{\pm}$, and the l-cycle σ_l is even, it acts non-trivially on $\sqrt{t}$, and hence the same holds for the Frobenius elements of $P^{\pm}$. This means that $t = \delta^{\pm}$ is never a square modulo $P^{\pm}$ in $\mathbf{F}_{q^2}$. On the other hand, $B^{+}(\lambda)$ is, and $B^{-}(\lambda)$ is not, a square in $\mathbf{F}_{q^2}$.

If the Galois group of $f^{\pm}$ over $\mathbf{F}_{q^2}(\sqrt{t})$ is S_l, then the fields $\mathcal{F}^{\pm}$ and $\mathbf{F}_{q^2}(\sqrt{t})$ are disjoint over $\mathbf{F}_{q^2}(t)$, and hence the Galois group of $\mathcal{F}^{\pm}(\sqrt{t})$ over $\mathbf{F}_{q^2}(t)$ equals $S_l \times \mathbf{Z}/2$, where the generator of $\mathbf{Z}/2$ acts like $\sqrt{t} \to -\sqrt{t}$. We can then apply Chebotarëv's theorem to the extension $\mathcal{F}(\sqrt{t})$ of $\mathbf{F}_{q^2}(t)$ to find primes $P^{\pm} = t - \delta^{\pm}$ of degree one in $\mathbf{F}_{q^2}(t)$ whose Frobenius elements act like $\sigma_l \times (-1)$ in $S_l \times \mathbf{Z}/2$. This means again that $\delta^{\pm}$ are non-squares in $\mathbf{F}_{q^2}$ and the corresponding statements about $B^{\pm}(\lambda)$ are satisfied. This proves the proposition. □

5. Proof of the corollaries

(5.1) *Proof of corollary 1.* From genus theory, we know that $\mathcal{C}$ is cyclic. The result then follows immediately from the well-known exact sequence

$$0 \to J[2^{\infty}](\mathbf{F}_q) \to \mathcal{C} \to \mathbf{Z}/d\mathbf{Z} \to 0,$$

where $d \in \{1,2\}$ is the degree of T^{-1} in $K(\sqrt{e\mathfrak{p}})$ (so $d=2$ if and only if k is even). □

(5.2) *Proof of corollary 2.* This follows from the formula in (2.2) since the type number $t(\mathfrak{p})$ of the quaternion algebra ramified at the finite prime $\mathfrak{p}$ of degree k equals $g(\mathfrak{p})$ (Gekeler, *loc. cit.*). Actually, for $4|\deg \mathfrak{p}$,

$$2|t(\mathfrak{p}) \iff \begin{cases} 8|h(e\mathfrak{p}) & \text{if } 8|k \\ 8\not|h(e\mathfrak{p}) & \text{if } 8\not|k \end{cases},$$

as follows from the formula for $g(\mathfrak{p})$ given in (2.2). □

Acknowledgments. The author is post-doctoral fellow of the Fund for Scientific Research - Flanders (FWO -Vlaanderen). This work was done while visiting the MPIM.

References

[1] S.B. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bull. A.M.S. **27** (1992), nr. 1, 68–133.

[2] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen, I, II*, Math. Z. **19** (1924), 153–246, = Collected Papers, pp. 1–94.

[3] P. Barrucand and H. Cohn, *Primes of type x^2+32y^2, class number and residuacity*, J. reine angew. Math. **238** (1969), 67–70.

[4] G. Cornelissen, *Zeros of Eisenstein series, quadratic class numbers and supersingularity for rational function fields*, Math. Ann. **314** (1999), 175–196.

[5] P. Lejeune-Dirichlet, *Collected works*, Chelsea Publ., New York, 1969.

[6] G. van der Geer and M. van der Vlugt, *Kloosterman sums and the p-torsion of certain Jacobians*, Math. Ann. **290** (1991), 549–563.

[7] E.-U. Gekeler, *Über Drinfeld'sche Modulkurven vom Hecke-Typ*, Compos. Math. **57** (1986), 219–236.

[8] W.D. Geyer and M. Jarden, *Bounded realization of l-groups over global fields. The method of Scholz and Reichardt*, Nagoya Math. J. **150** (1998), 13–62.

[9] T. Hansen and G.L. Mullen, *Primitive polynomials over finite fields*, Math. Comp. **59** (1992), 639–643.

[10] H. Hasse, *Über die Klassenzahl des Körpers $P(\sqrt{-p})$ mit einer Primzahl $p \equiv (1 \bmod 2^3)$*, Aequationes Math. **3** (1969), 231–234.

[11] D.R. Hayes, *Explicit class field theory in global function fields*, in: Studies in Algebra and Number theory (ed. G.C. Rota), Advances in Math. Suppl. Stud. **6** (1979), Academic Press, New York-London, pp. 173–217.

[12] P. Kaplan, *Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan **25** (1973), 596–608.

[13] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[14] P.M. Neumann, *Some primitive permutation groups*, Proc. London Math. Soc. **50** (1985), 265–281.

[15] L. Rédei, *Ein neues zahlentheoretisches Symbol mit Anwendungen auf die Theorie der quadratischen Zahlkörper*, J. reine angew. Math., **180** (1939), 1–43.

[16] J.-P. Serre, *Corps locaux*, Actualités scientifiques et industrielles, vol. 1296, Hermann, Paris, 1968.

[17] P. Stevenhagen, *Divisibility by 2-powers of certain quadratic class numbers*, J. Number Theory **43** (1993), no. 1, 1–19.

[18] H. Wielandt, *Finite Permutation groups*, Werke, vol. I, de Gruyter, Berlin - New York, 1994, pp. 119–198.

Max-Planck-Institut für Mathematik, Gottfried-Claren-Straße 26, D-53225 Bonn *(current)*

University of Gent, Dept. of Pure Mathematics, Galglaan 2, B-9000 Gent

e-mail: `gc@cage.rug.ac.be`